

Regarding a Representation-Theoretic Conjecture of Wigderson

Cristopher Moore
Computer Science Department
University of New Mexico
and the Santa Fe Institute
moore@cs.unm.edu

Alexander Russell
Computer Science and Engineering
University of Connecticut
acr@cse.uconn.edu

September 22, 2010

Abstract

We show that there exists a family of irreducible representations ρ_i (of finite groups G_i) such that, for any constant t , the average of ρ_i over t uniformly random elements $g_1, \dots, g_t \in G_i$ has operator norm 1 with probability approaching 1 as $i \rightarrow \infty$. This settles a conjecture of Wigderson in the negative.

1 Introduction

There are known families of finite groups, such as $\text{SL}_2(\mathbb{F}_p)$ as $p \rightarrow \infty$, which yield expanding Cayley graphs over a constant number of uniformly random group elements g_1, \dots, g_t [2]. In particular, for any nontrivial irreducible representation ρ of such a group, the expectation of ρ over the g_i has operator norm bounded below 1:

$$\mathbb{E}_{\{g_1, \dots, g_t\}} \left[\left\| \frac{1}{t} \sum_{i=1}^t \rho(g_i) \right\|_{\text{op}} \right] \leq 1 - \varepsilon, \quad (1)$$

where $t > 1$ and $\varepsilon > 0$ are constants depending only on the group family.

A conjecture of A. Wigderson states that there are universal constants t and $\varepsilon > 0$ such that (1) holds for any group G and any nontrivial irrep $\rho \in \widehat{G}$. This would imply that for each ρ , a constant number of random elements make G “act like an expander” with respect to ρ , and therefore that $O(\log |\widehat{G}|)$ random elements suffice to turn G into an expander. This holds, in particular, for abelian groups: while no constant number of elements suffice to make \mathbb{Z}_2^n into an expander, or even to generate the entire group, just $t = 2$ elements suffice to bound the expected norm of any one irrep, with a universal constant $\varepsilon > 0$.

Our strategy will be to work in a family of finite groups of the form $G = K^n$. Such groups simultaneously possess high-dimensional representations and the property that any collection of a constant number of group elements generate a subgroup of constant size. We then show that a representation ρ selected at random according to the Plancherel distribution contains a copy of the trivial representation when restricted to almost all relevant small subgroups. This implies that, with high probability in the random elements g_1, \dots, g_t , the expectation of ρ over these elements has operator norm 1.

Our proof focuses on the random variable

$$X_H = \frac{\langle \text{Res}_H \chi_\rho, 1 \rangle_H}{d_\rho}, \quad (2)$$

where H is a fixed subgroup of a group G and ρ is selected according to the Plancherel measure. Since X_H is the dimensionwise fraction of ρ that restricts to the trivial representation under H , whenever $X_H > 0$ we have

$$\left\| \mathbb{E}_{h \in H} \rho(h) \right\|_{\text{op}} = 1.$$

We will show that for groups of the form K^n , if $H = \langle g_1, \dots, g_t \rangle$ then $X_H > 0$ with high probability. We do this by computing the first two moments of X_H , first for general group-subgroup pairs, and then specializing to the groups K^n .

Notation; actions on the group algebra Given a finite group G , let \widehat{G} denote its set of irreducible representations ρ , let $\chi_\rho(g) = \text{tr } \rho(g)$ denote their characters, and let $d_\rho = \chi_\rho(1)$ denote their dimensions. Let $\mathbb{C}[G]$ denote the group algebra on G . The left action of G on $\mathbb{C}[G]$ obtained by linearly extending the rule $g : g' \mapsto gg'$ induces the *regular representation* of G with character

$$R(g) = \begin{cases} |G| & \text{if } g = 1, \\ 0 & \text{otherwise.} \end{cases}$$

As a consequence of character orthogonality, one can express R as the sum

$$R = \sum_{\rho \in \widehat{G}} d_\rho \chi_\rho.$$

The algebra $\mathbb{C}[G]$ can likewise be given the structure of a $G \times G$ representation by linearly extending the rule $(g_1, g_2) : g \mapsto g_1 g g_2^{-1}$. The character B of this representation thus satisfies

$$B(g_1, g_2) = |\{g : g_1 g g_2^{-1} = g\}|.$$

Again applying character orthogonality, B can be expressed as the sum

$$B(g_1, g_2) = \sum_{\rho \in \widehat{G}} \chi_\rho(g_1) \cdot \chi_\rho^*(g_2).$$

Finally, the Plancherel measure \mathcal{P} on \widehat{G} assigns each representation τ the probability mass

$$\mathcal{P}(\rho) = \frac{d_\rho^2}{|G|}.$$

Returning now to the random variable X_H defined above, we compute its first two moments.

2 The first two moments

The expectation For the first moment, observe that if $\rho \in \widehat{G}$ is distributed according to the Plancherel measure, then

$$\begin{aligned} \mathbb{E}_\rho X_H &= \mathbb{E}_\rho \frac{\langle \text{Res}_H \chi_\rho, 1 \rangle_H}{d_\rho} = \sum_\rho \frac{d_\rho^2}{|G|} \frac{\langle \text{Res}_H \chi_\rho, 1 \rangle_H}{d_\rho} = \frac{1}{|G|} \sum_\rho d_\rho \langle \text{Res}_H \chi_\rho, 1 \rangle_H \\ &= \frac{1}{|G|} \left\langle \text{Res}_H \sum_\rho d_\rho \chi_\rho, 1 \right\rangle_H = \frac{1}{|G|} \langle \text{Res}_H R, 1 \rangle_H = \frac{1}{|H|}. \end{aligned}$$

The second moment For the second moment, observe that

$$\begin{aligned}\mathbb{E}_\rho X_H^2 &= \sum_\rho \frac{d_\rho^2}{|G|} \frac{\langle \text{Res}_H \rho, 1 \rangle_H^2}{d_\rho^2} = \frac{1}{|G|} \sum_\rho \langle \text{Res}_{H \times H} \chi_\rho \times \chi_\rho^*, 1 \rangle_{H \times H} \\ &= \frac{1}{|G|} \langle \text{Res}_{H \times H} B, 1 \rangle_{H \times H} = \frac{1}{|G|} \frac{1}{|H|^2} \sum_{h_1, h_2 \in H} |\{g : h_1^{-1} g h_2 = g\}|.\end{aligned}$$

Thus

$$\begin{aligned}\text{Var}_\rho[X_H] &= \mathbb{E}_\rho X_H^2 - \frac{1}{|H|^2} = \frac{1}{|H|^2} \left(\sum_{(h_1, h_2) \in H \times H} \Pr_g[h_1 = g^{-1} h_2 g] - 1 \right) \\ &= \frac{1}{|H|^2} \sum_{\substack{(h_1, h_2) \in H \times H \\ (h_1, h_2) \neq (1, 1)}} \Pr_g[h_1 = g^{-1} h_2 g] = \frac{1}{|H|^2} \sum_{\substack{h \in H \\ h \neq 1}} \frac{|h^G \cap H|}{|h^G|} \leq \frac{1}{|H|} \sum_{\substack{h \in H \\ h \neq 1}} \frac{1}{|h^G|},\end{aligned}$$

where $h^G = \{g^{-1} h g : g \in G\}$ is the conjugacy class of h in G .

Applying Chebyshev's inequality, we conclude that

$$\Pr_\rho[X_H = 0] \leq \Pr \left[\left| X_H - \frac{1}{|H|} \right| \geq \frac{1}{|H|} \right] \leq |H| \sum_{\substack{h \in H \\ h \neq 1}} \frac{1}{|h^G|}. \quad (3)$$

3 Groups of the form $G = K^n$ and the main theorem

We consider now the groups $G = K^n$, where K is a finite group with no center. We will prove the following.

Theorem 1. *Let K be a finite group with center $\{1\}$ and let $G = K^n$. Let t be such that $2|K|^t \leq \alpha\sqrt{n}$, let $\mathbf{h}_1, \dots, \mathbf{h}_t$ be independent elements selected uniformly from G , and let $\rho = \rho_1 \otimes \dots \otimes \rho_n$ be chosen according to the Plancherel measure on \widehat{G} . Then*

$$\Pr_{\rho, \{\mathbf{h}_i\}} [X_H = 0] \leq \frac{2\alpha}{\sqrt{n}} + \left(2^{-1/\alpha} |K|^\alpha \right)^{\sqrt{n}},$$

where H is the subgroup generated by the elements $\mathbf{h}_1, \dots, \mathbf{h}_t$ and X_H is defined as in (2). It follows that there exists a representation $\rho = \rho_1 \otimes \dots \otimes \rho_n$ so that

$$\Pr_{\{\mathbf{h}_i\}} \left[\left\| \frac{1}{t} \sum_i \rho(\mathbf{h}_i) \right\|_{\text{op}} < 1 \right] \leq \frac{2\alpha}{\sqrt{n}} + \left(2^{-1/\alpha} |K|^\alpha \right)^{\sqrt{n}}.$$

If $\mathbb{E}_{\mathbf{h} \in H} \|\rho(\mathbf{h})\|_{\text{op}} = 1$, then certainly $\mathbb{E}_{\{\mathbf{h}_i\}} \|\rho(\mathbf{h}_i)\|_{\text{op}} = 1$. Thus, with high probability in the group elements $\{\mathbf{h}_i\}$, almost all representations ρ have norm 1 when averaged over the \mathbf{h}_i , where “almost all” is defined with respect to the Plancherel measure.

Note that for any fixed K , there is an $\alpha > 0$ such that $\Pr[X_H = 0] = o(1)$. Thus in order to bring the expected norm of ρ down to $1 - \varepsilon$ for any constant $\varepsilon > 0$, we need $t = \Omega(\log n) = \Omega(\log \log |G|)$ random elements. Compare this to the Alon-Roichman theorem [1], which states that $O(\log |G|)$ random elements suffice with high probability to bound the norm of *every* irrep ρ , and thus turn G into an expander. We have not attempted to close this gap.

Anticipating the proof, we collect a few facts about subgroups of K^n . Let $\pi_i : K^n \rightarrow K$ be the homomorphism that projects onto the i th coordinate of K^n . For a sequence $\mathbf{h}_1, \dots, \mathbf{h}_t$ of t elements of K^n , define the function $\mathbf{s} : \{1, \dots, n\} \rightarrow K^t$ by the rule

$$\mathbf{s}(i) = (\pi_i(\mathbf{h}_1), \dots, \pi_i(\mathbf{h}_t)).$$

Observe that if $\mathbf{s}(i) = \mathbf{s}(j)$ then the i th and j th coordinates of any product of the \mathbf{h}_i are identical.

Lemma 1. *Let H be the subgroup of K^n generated by t elements $\mathbf{h}_1, \dots, \mathbf{h}_t$. Then $|H| \leq |K|^{|K|^t}$.*

Proof. As K^t has cardinality $|K|^t$, the coordinates of K^n can be partitioned into no more than $|K|^t$ sets, each of which is constant for any product of the \mathbf{h}_i . It follows that they generate a group of size no more than $|K|^{|K|^t}$. \square

For an element $\mathbf{g} = (g_1, \dots, g_n) \in K^n$, let $\text{supp}(\mathbf{g}) = |\{i : g_i \neq 1\}|$ denote the size of the support of \mathbf{g} . We extend the definition to subgroups: for a subgroup $H < K^n$, define

$$\text{supp}(H) = \min_{\substack{\mathbf{h} \in H \\ \mathbf{h} \neq \mathbf{1}}} \text{supp}(\mathbf{h}).$$

While the exact relationship between $\text{supp}(H)$ and its generators may be complicated, we can give a lower bound for $\text{supp}(H)$ in terms of the partition formed by the function \mathbf{s} defined above. Specifically, for a sequence of elements $\mathbf{h}_1, \dots, \mathbf{h}_t$, let

$$d = d(\mathbf{h}_1, \dots, \mathbf{h}_t) = \min_{\mathbf{s} \in K^t} |\{i : \mathbf{s}(i) = \mathbf{s}\}|$$

denote the size of the smallest set in the partition, and observe that if \mathbf{h} is a product of some sequence of the \mathbf{h}_i not equal to $\mathbf{1}$, then $\text{supp}(\mathbf{h}) \geq d$. In particular, if H is the subgroup generated by the \mathbf{h}_i , we have $\text{supp}(H) \geq d(\mathbf{h}_1, \dots, \mathbf{h}_t)$.

Lemma 2. *Let $\mathbf{h}_1, \dots, \mathbf{h}_t$ be t uniformly random elements of K^n . Then*

$$\Pr \left[d(\mathbf{h}_1, \dots, \mathbf{h}_t) \leq \frac{n}{2|K|^t} \right] \leq \frac{4|K|^{2t}}{n}.$$

Proof. For a given element $\mathbf{s} \in K^t$, let $X_{\mathbf{s}}$ be the random variable equal to the size of the corresponding set in the partition, $\{i : \mathbf{s}(i) = \mathbf{s}\}$. Since $X_{\mathbf{s}}$ is binomially distributed as $\text{Bin}(n, 1/|K|^t)$, we have $\mathbb{E}X_{\mathbf{s}} = n/|K|^t$ and $\text{Var}X_{\mathbf{s}} \leq n/|K|^t$. By Chebyshev's inequality,

$$\Pr \left[\left| X_{\mathbf{s}} - \frac{n}{|K|^t} \right| \geq \frac{n}{2|K|^t} \right] \leq \frac{4|K|^{2t}}{n}.$$

Since there are $|K|^t$ elements of K^t , the union bound implies the statement of the lemma. \square

Note that the random variable $X_{\mathbf{s}}$ obeys the Chernoff bound, making it much more concentrated than the second moment calculation we did here suggests, but this is not important to our results.

We finally return to the proof of Theorem 1.

Proof of Theorem 1. Let $\mathbf{h}_1, \dots, \mathbf{h}_t$ be t elements chosen independently and uniformly at random from K^n , and let H denote the subgroup they generate. Additionally, let $\rho = \rho_1 \otimes \dots \otimes \rho_n$ be a representation of K^n selected according to the Plancherel measure. Then with $d = d(\mathbf{h}_1, \dots, \mathbf{h}_t)$ as above,

$$\begin{aligned} \Pr_{\rho, \{\mathbf{h}_i\}} [X_H = 0] &\leq \Pr_{\{\mathbf{h}_i\}} \left[d < \frac{n}{2|K|^t} \right] + \Pr_{\rho, \{\mathbf{h}_i\}} \left[X_H = 0 \mid d \geq \frac{n}{2|K|^t} \right] \\ &\leq \frac{4|K|^{2t}}{n} + \max_{\substack{\{\mathbf{h}_i\} \text{ such that } \\ d \geq n/2|K|^t}} \Pr_{\rho} [X_H = 0], \end{aligned} \quad (4)$$

the second line following from Lemma 2.

As K has no center, any nontrivial element $g \in K$ has at least two conjugates. In particular, the centralizer $Z_g = \{h \mid g = h^{-1}gh\}$ is a proper subgroup of K . It follows that for an element $\mathbf{h} \neq 1$ of K^n the conjugacy class \mathbf{h}^{K^n} has cardinality $|\mathbf{h}^{K^n}| \geq 2^{\text{supp}(\mathbf{h})}$. If $d \geq n/2|K|^t$, then $\text{supp}(H) \geq n/2|K|^t$ and

$$|H| \sum_{\mathbf{h} \neq 1} \frac{1}{|\mathbf{h}^{K^n}|} \leq |H|^2 2^{-\text{supp}(H)} \leq |K|^{2|K|^t} 2^{-n/2|K|^t},$$

by Lemma 1. Writing $2|K|^t \leq \alpha\sqrt{n}$, we have

$$|H| \sum_{\mathbf{h} \neq 1} \frac{1}{|\mathbf{h}^{K^n}|} \leq \left(2^{-1/\alpha} |K|^\alpha \right)^{\sqrt{n}}.$$

Combining equations (3) and (4) gives

$$\Pr_{\rho, \{\mathbf{h}_i\}} [X_H = 0] \leq \frac{2\alpha}{\sqrt{n}} + \left(2^{-1/\alpha} |K|^\alpha \right)^{\sqrt{n}},$$

completing the proof. □

References

- [1] Noga Alon and Yuval Roichman. Random Cayley graphs and expanders. *Random Struct. Algorithms*, 5(2):271–285, 1994.
- [2] Jean Bourgain and Alexander Gamburd. On the spectral gap for finitely-generated subgroups of $\text{SU}(2)$. *Inventiones Mathematicae*, 171:83–121, 2008.